Article

Governing Proliferation in Cybersecurity

Trey Herr*
Belfer Center's Cyber Security Project at the Harvard Kenned School and Non-Resident Fellow with New America's Cybersecurity Initiative

This article compares state activities to control the international spread of malware with efforts to counter the proliferation of weapons of mass destruction (WMD). The analysis focuses on representative institutions, the Wassenaar Arrangement (Wassenaar) which began to address malware in 2013, and the Proliferation Security Initiative (PSI), comparing the origins, operation, and relative success of each. The article challenges the idea that PSI might serve as a successful model for countering malware proliferation, examining several basic questions about governing proliferation to offer insight into cybersecurity for the research and practitioner community. Looking at both intentional proliferation, through alliances, proxy relationships, or the malware markets, and unintentional proliferation, the article outlines key ideas in cybersecurity and underlines the challenges to governance. Concluding, the article argues PSI is a poor model to address malicious software, but that there are two substantive goals which may see more success: creating legal protections for cybersecurity research; and limiting the supply of software vulnerabilities available to attackers. Highlighting these differences between the approaches of Wassenaar and the PSI, this article presents cybersecurity as an interdependent ecosystem of people and ideas suitable for examination rather than being inaccessible or a purely technical space

Introduction

Cybersecurity can be seen by scholars as holding an air of technical mysticism and opacity. In truth, it is a very human space and understanding the interplay of attack and defense with malicious software entails understanding as much about the people and organizations at play as the code moving between computers. Understanding cybersecurity, however foreign or technically remote it may seem, is both possible and important.

In 2015, China and the U.S.A. agreed to restrict their espionage activities targeting each other's commercially valuable information. The agreement was hailed as major progress in demarcating the boundaries of acceptable behavior in an important area of cybersecurity (Zucker 2015). The two nations agreed in principle on several behaviors including commitments to provide timely information on malicious activities, refrain from conducting or knowingly supporting the theft of intellectual property, and to support efforts to identify and promote appropriate norms in cyberspace (Rollins 2015). The US–China agreement was one of the most prominent in the past half-decade to govern state's responsibilities around their activities in cyberspace, but it was not the only one.

Through several yearlong rounds between 2010 and 2017 the United Nation's First Committee—dealing with arms control and international

*Send correspondence to Trey Herr, Fellow at the Belfer Center's Cyber Security Project at the Harvard Kenned School and Non-Resident Fellow with New America's Cybersecurity Initiative. E-mail: Trey_Herr@hks.harvard.edu

© The Author 2017. Published by Oxford University Press on behalf of Munk School and Rotman School of Management. All rights reserved. For permissions, please e-mail: journals.permissions@oup.com
doi: 10.1093/global/gux006 Advance Access publication 3 July 2017

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

security—has organized a meeting of governments to examine state behavior and cooperation in cybersecurity, the Group of Government Experts (GGE). The 2016–2017 round of this GGE process addresses the spread of malicious software in cybersecurity as a concern for international peace and stability. Even prior to the GGE, in 2013, the Wassenaar Arrangement, a voluntary export control harmonization body, added controls which restrict the sale of software used for surveillance and malicious activities (Anderson 2015).

What was evident from each of these efforts was the expression of intent that states be involved in governing malicious activities in cyberspace, including that of other states. Previous agreements, most notably the Budapest Convention which focused on cyber crime, targeted non-state groups in an effort to shape international consensus without explicitly debating state behavior. China's campaign to siphon intellectual property and national security information from U.S.A. was part of a broad economic strategy by the state. Addressing this behavior directly opens the door for broader discussions as to the ways states govern their behavior in cybersecurity.

What is behind these efforts by states to extend governance to cybersecurity? More than applying yesterday's norms to tomorrow's technology, the use of export controls to govern the sale of malware is a manifestation of states' interest in managing the national security implications of cybersecurity. Failure to recognize this motivation clouds scholarship and muddles debate. Policy practitioners, as well as the scholars who interact with them and study cybersecurity, need to have a coherent set of concepts for evaluating state governance behaviors. Otherwise, the quality of debate declines, and relevance of necessary scholarship diminishes. This article compares the origin of two proliferation-focused regimes, Wassenaar's controls on malicious software, and the Proliferation Security Initiative (PSI), a voluntary group of states which coordinates the interdiction of weapons of mass destruction (WMD) and related technologies.

Both Wassenaar and the PSI are focused on the transfer of controlled components and technology but they deal with vastly different subject matter. This article compares their respective origins and functionality, considering proposals by some to advance international cybersecurity cooperation under a new PSI-like model (International Security Advisory Board 2014). Starting with a description of the two proliferation regimes, the section "Background" provides background on Wassenaar and the PSI to establish this central comparison. The section "Defining the Content of Proliferation" looks at each regime's definition and the goods being proliferated. This section also looks at how these goods are developed. "Contrasting Proliferation Processes" explores how these good proliferate, describing some of the key processes and networks in play. The section "The Goals of Governing Proliferation" looks at goals a state might have in governing proliferation under each of these regimes while the section "Conclusion" provides concluding thoughts. While the PSI is an interesting model for WMD components, its light legal touch and focus on limiting the transfer of devices and technology does not appear likely to function well in targeting malicious software. Indeed, the origin of the PSI's features provide little emphasis on building consensus on *what* is being controlled, focusing rather on facilitating existing interdiction activities. As a model of policy innovation, the PSI may represent a highly abstracted model to generating consensus between parties but would have little concrete positive impact.

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

Background

The Wassenaar Arrangement

Wassenaar is an export control regime founded in 1996 by U.S.A. and a group of Western and former Eastern bloc states. Wassenaar replaced a Cold War era export control agreement known as the Coordinating Committee for Multilateral Export Controls, or CoCom. CoCom united Western countries to restrict the sale of advanced commercial and some military products to the Warsaw Pact countries (Mastanduno 1992). Wassenaar was constructed with an intention to be more inclusive than CoCom and in fact counts former Soviet satellites as members. Wassenaar eventually grew from 30 to 41 states including the U.K., Italy, Germany, and the Russian Federation. Though Israel is not a member it has implemented laws to match those of Wassenaar. Although it has no direct enforcement authority and is without binding restrictions, Wassenaar serves as a voluntary mechanism for states to coordinate their domestic export control policies (Lipson 1999). Wassenaar provides a common basis for states to identify items to be restricted through export laws and prevent regulatory arbitrage, where companies move to the most permissive jurisdiction in which to offer their products. Wassenaar maintains a series of control lists focused on both military and dual-use technologies. Member states can suggest changes which are then subject to an agreement by consensus. Each country is then responsible for implementing changes to their domestic law upon the adoption of new or modified controls.

Wassenaar was first used to target cryptographic software during the 1990s in a failed attempt to limit the international diffusion of this software designed to mathematically obscure data like emails and documents. Despite Wassenaar's lack of success against cryptography, it became the vehicle of choice to restrict the proliferation of malware. Prior to Wassenaar's 2013 annual meeting, the U.K. and French governments proposed to change the control lists and add new rules covering the tools and technology associated with malicious software (Anderson 2015). The choice to adapt Wassenaar, instead of developing a new standalone agreement or treaty acknowledged the difficulty building consensus around the key problems in cybersecurity governance, especially the flow of software and information across borders. It also raised the issue of proliferation—a new topic for cybersecurity, but one well understood in the broader security community.

The Proliferation Security Initiative

The PSI was developed in 2003, led by U.S.A. to overcome a perceived gap in international law which prevented the search and seizure of some vehicles suspected of carrying WMD components. At its core is the Statement of Interdiction Principles which, though short, emphasizes the role of each member state's domestic law in determining the scope of action and the importance of sharing information. The PSI is entirely voluntary, without legally binding authority, a secretariat, or any coordinating body. Its core principles do not include specification of the goods to be controlled so what states determine to be covered by the PSI can vary widely. Indeed, the only requirement of a member state is to endorse the Principles. What started as U.S.A. and ten allies has grown to more than a hundred countries (though without the involvement of nuclear states like China, Pakistan, and India

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

and the then near breakout South Africa). Where there are questions of law countries are directed to the United Nations Security Council and any pertinent directives covering the behavior of a target state like North Korea or Libya. The PSI has operated with moderate success for more than a dozen years, though with criticism, owing to the limited scope and non-binding nature of the Principles (Koch 2012; Williams 2013). There have been several prominent interdictions by states participating in the PSI but it is difficult to tell if these would not have taken place absent the regime. (Durkalec 2012; Dunne 2013).

A Modern Model of Governance

In debating the governance of cybersecurity, especially the international sale and transfer of malicious software used to break into computer systems, analysts' rhetoric often quickly invokes the specter of arms control (Arimatsu 2012; Bronk and Wallach 2013; King and Litwak 2015). But arms control is a poor framework for controlling malware as it deals more with qualitative i.e., what kind or quantitative, how many restrictions on weapons systems. Malware cannot be counted as a weapon system or categorized so neatly as, for instance, ballistic missiles with one warhead versus ten. Fissile material critical to the construction of a nuclear weapon is naturally scarce and has telltale signature in the various flavors of radiation. This material is hard to locate and difficult to transport.

It appears to be a mistake to try to restrict malicious software using the same policy tools as have been applied to the theft of nuclear materials, or applied to trade in chemical weapons. Perhaps as important, efforts to control the spread of nuclear arms started when there was a small (and so relatively tractable from the standpoint of an international agreement) number of states with the weapons. Blocking the spread of these capabilities to new states outright was challenging but made simpler by the limited number of 'haves' and comparatively large number of 'have-nots'. The private sector plays a substantial role in cybersecurity. Companies like Google and Microsoft build the software which serves as the contested ground between attacker and defender. Many of these same companies, alongside communities of researchers and non-profits, help set the standards for how the web is built (Mueller 2004; DeNardis 2014). Criminal groups across a range of skill levels develop and deploy malicious software to manipulate computer systems. In cybersecurity, the 'haves' are everywhere.

Pathway to Proliferation: Wassenaar and the PSI

An alternative framing, used by the European Union (EU) in a recent export control proposal as well as by the UN GGE, is proliferation – the diffusion of capabilities and acquisition by different actors (Lewis and Kerstin 2016). These efforts may focus on non-proliferation, attempts to prevent the acquisition of capabilities by actors, e.g., by blocking the acquisition of weapons or critical resources like fissile material to a state. They could also be framed as counter-proliferation which, by contrast, aims to reduce the utility of capabilities already in the hands of actors (Larsen and Smith 2005). This can be as simple as interdiction operations to limit the flow of sustaining materials and technology for a weapon or more direct efforts to cripple delivery

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

systems and introduce uncertainty in their use (Anderson, Devine, and Gibbons 2014).

Wassenaar is the first international vehicle used to restrict the proliferation of malware as opposed to crime or other activities more broadly but it is not the last and this move toward addressing proliferation in cybersecurity has spawned comparisons to previous non- and counter-proliferation agreements. A prominent example of this turn to proliferation analogies is the idea to model a response in cybersecurity along the lines of the PSI (Castelli 2014; Sterner 2015; Lewis and Kerstin 2016). Developed to interdict the spread of WMD devices, as noted above, the PSI has occupied a central role in the discussion over proper analogies for cybersecurity and proliferation, most prominently through informal proposals by some in the U.S. State Department. While research has discussed the nuclear to cyber analogy, less work has compared the resulting governance regimes (Shackelford 2009; Nye 2011; Goldman and Arquilla 2014).

The PSI has seen some success, with U.S.A. able to leverage the membership of states like Panama and the Marshall Islands as a basis to claim the interdiction of several dozen vessels between 2005 and 2006 (Belcher 2011). While it is difficult to count incidents which could only have taken place under the PSI's principles, the PSI has also encouraged a number of international exercises and more effective in-port seizures of WMD components by member states (Dunne 2013). Wassenaar, by contrast, has seen substantial turmoil since adding the tools and technology related to malicious software (labeled "intrusion software") in 2013 (Bratus et al. 2014; Little Limbago and Pierce 2015). This is in part because, unlike WMD components, the nature of malicious software does not lend itself well to transfer-focused controls.

Defining the Content of Proliferation

What is malware and how do these governance regimes define the things they are attempting to control? For the PSI, there is a loose consensus around what constitutes WMD devices and a larger debate over what should be counted as a related component. This consensus, such as it is, leaves room for differences in interpretation by member states. Wassenaar targets a much more specific topic, malicious software, and indeed only restricts the tools and technology used to create or communicate with this malware rather than the software itself. A starting point, therefore, is to examine the different goods targeted by these proliferation regimes.

The PSI: Targets for Interdiction

The PSI is designed to interdict the flow of WMD and supporting dual use goods. Importantly, the PSI leaves this definition of what constitutes WMD or related devices entirely in the hands of member states. This makes for a broad span of possible items, from nuclear weapons components to civilian machine tools with potential defense application. In addition to weapons and related components, the PSI is also concerned with delivery systems, missile components, and high-strength materials which could be used to produce them (Nikitin 2012). Looking at nuclear weapons for instance, interdiction could take place to stop materials anywhere in the nuclear lifecycle from highly enriched uranium to the aluminum tubing used in

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

centrifuges and enrichment processes. Some notable PSI actions have targeted shipments of intermediate range SCUD missiles from North Korea (DPRK) to Yemen and centrifuge components being transported from Malaysia to Libya via a German flagged carrier (Belcher 2011).

In many cases, interdiction takes place to stop a component or critical resource in the development of some WMD device e.g., enriched uranium or the centrifuge pieces bound for Libya. The PSI thus targets a weak point in the proliferation cycle: as states and other groups try to covertly assemble these complex technical systems, they must move delicate machinery and materials across the world. A.Q. Khan, a Pakistani nuclear physicist responsible for establishing that country's uranium enrichment program, was also behind an international network that transferred critical expertise, machinery, and radioactive material to Libya, Iran, and the DPRK. Each of these states depended on the Khan network at some stage of their construction of a nuclear weapons program (Corera 2006; MacCalman 2016).

What Is Malware?

Malware, by contrast, requires no special materials or machinery. A key issue in cybersecurity is that controlling the transfer of software amounts to controlling the transfer of information. This is a difficult proposition, especially when the software attackers might employ is also useful to the defensive community. Malicious software is information—software code—which works to manipulate a computer system or network. That manipulation might just steal a user's passwords or could create physical damage. To gain access to a computer system, malware typically needs a means of moving from its creators to the target. This propagation from A to B could be highly specific, like e-mail to one person, or broad in nature, distributed through a viral meme on social media (Herr 2014). The resources and infrastructure required to send this e-mail could involve compromising computer systems in many intermediary countries, unrelated to the malware's origin or its target. These sort of multistage campaigns are not uncommon, especially for high-value targets (Ramilli and Bishop 2010; Haq et al. 2013; Kogan 2015).

Once on a target computer, malware must be able to run just like any other kind of software. *Unlike* what you might download from Microsoft however, malicious software cannot just ask the target's permission to run. Instead it must trick the system. A user might be presented with a PDF file, attached to an e-mail with instructions to open it and view the contents. By clicking on the document, the user triggers an exploit. This exploit is a software program which takes advantage of a vulnerability, a badly designed feature, or flaw in the user's computer, to gain access. These exploits, though not required for all forms of malware, are relatively common and often represent well known holes in software or security systems that remain unfixed [Data Breach Investigations Report (DBIR) 2015]. In a very small number of instances, an attacker working against a computer with no well-known or easy to target flaws might employ a zero-day or exploit which takes advantage of a vulnerability unknown to the user or their software's creator.

Once on a computer system, the attacker needs to deploy malware to execute and achieve some specific end like stealing credit card information or disrupting a piece of attached hardware like a power turbine. This portion of the malware is known as the payload and is the clearest expression of malware's intent—what the creator wishes to do to a target is embedded in

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

how this payload is written (Herr and Rosenzweig 2015). More capable examples of malware often modularize these payloads, spreading out the responsibility for different functions to separate small programs working in concert. Stealing a document may be comparatively easy since copying and moving a file is standard behavior for an operating system. Writing a payload to cause a computer to damage itself or sending a series of commands to connected hardware like a power turbine to have it destroy itself requires more intimate knowledge of the targeted software's design.

Definitions

The PSI is vague on what it controls, leaving it to member states to specify. In U.S.A., for example, WMD are defined to include radioactive devices and chemical weapons as well as more pedestrian items like mines, grenades, and rockets with more than four ounces of propellant (18 U.S. Code § 2332a—"Use of weapons of mass destruction" and 18 U.S. Code § 921—"Definitions").

Wassenaar, by contrast, attempts to establish a high degree of precision in identifying software by design and function. Wassenaar covers "intrusion software" which is defined as "'Software' specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures', of a computer or network-capable device, and performing any of the following: [a] The extraction of data or information, from a computer or network capable device, or the modification of system or user data or [b] The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions".

Wassenaar does not control this intrusion software directly but rather any products, software, and technology used to support, develop, maintain, or communicate with it. Many of the terms in this definition have become flashpoints for debate over Wassenaar and its approach to governing malicious software (Bratus et al. 2014; Dullien, Iozzo, and Tam 2015). The degree of detail being placed into the definition of *what* is to be controlled matters. Less specific approaches, like the PSI, can help bring in a broader array of states to participate in interdiction, lowering the barrier to entry. More detailed definitions might allow for countries to import the control whole cloth into their domestic law and create uniform restrictions and prevent regulatory arbitrage, but can also raise opposition from these domestic constituencies.

Why does this opposition matter? The same software and information an attacker might use to assemble a piece of malware is also regularly used by defenders in cybersecurity where the private sector plays an important role. This is somewhat like the use of radioactive material in civilian nuclear power facilities or chemicals which can be used to create pesticides and chemical weapons—but with an important caveat. In both of those examples the civilian use can be relatively well specified, with the chemicals and nuclear material each playing a well-established role in their respective processes. In cybersecurity, by contrast, the potential uses for malware and related information are wide-ranging. A software vulnerability by defenders may identify flaws and help build patches, or by attackers gain and maintain access to a computer system. In the late 1990s, companies began to buy these vulnerabilities from outside researchers through so-called bug bounty programs (Wilson et al. 2016). The result was transactions which rewarded

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

people for breaking vendor's software but also helped drive this vulnerability information to companies to fix these flaws. This question of what a software vulnerability plays an important role in understanding cybersecurity.

Vulnerabilities to Exploits

Flaws and mistakes in software are common. These flaws can often constitute a vulnerability which allows a third party to manipulate the underlying software. For example, a program that tries to retrieve an image file but fails to check what it found was indeed an image might retrieve a software program instead. Retrieving the image was intentional but failing to check the file which came back allows a third party to manipulate the computer.[1] Vulnerabilities may also be introduced directly to hardware, through bad design choices or deliberate compromises in chip manufacture somewhere along the supply chain (Becker et al. 2013; O'Neill 2016). The result is that many vulnerabilities exist in software around the world something akin to a natural resource waiting to be mined.

Vulnerabilities are embedded in software but they must also be discovered to be used. Once found, the discoverer must write an "exploit" to prove the vulnerability exists. The accepted way to demonstrate a vulnerability is to provide what is called a proof-of-concept (PoC) exploit, distributed as a way to show off an individual's skills, or communicate the vulnerability to a vendor (Espinoza 2016). These PoCs differ, sometimes quite radically, from the exploits used in malware however. The latter needs to be reliable across a range of different system configurations and better optimized to avoid detection by security software.[2] Where a PoC is scratched together to show a vulnerability exists, often by crashing the program in question, a production exploit would need to manipulate that same software without being detected (Ablon and Bogart 2017). The engineering in between a vulnerability and an exploit may involve multiple steps in design, discovery, and programming.

Importantly, exploits are not intrinsically malicious, they have an array of potential uses in the security industry. Vulnerability discovery, so-called 'bug-hunting', can be a factor of luck but much more commonly requires a great deal of time and skill. In part, this is because not all vulnerabilities are equal. In fact, these vulnerabilities may be present in parts of software which are relatively innocuous, or, these vulnerabilities may be present in parts of the software that are quite critical.[3] Part of a vulnerability's value is its secrecy: the term zero-day indicates a vulnerability which has existed in software since its release, so called for giving vendors no time to respond or develop a fix. As a result these previously unknown vulnerabilities are

[1] *In 2000, the Love Letter virus relied on exactly this flaw, where Windows 2000 and Windows XP would hide known extensions when reading file names from the right to the left. The Love Letter virus was a piece of malware which would execute if the user clicked on it. In this case, the malware was written in a language called Visual Basic so the extension for its file was ".vbs". But a user might be suspicious of a file with the ".vbs" extension, knowing it could be a software program. So, the malware file (LOVE-LETTER-FOR-YOU.TXT.vbs) hid itself by putting the (.vbs) outside of a benign extension (.txt) so Windows would only show .txt and the user would be none the wiser (Microsoft 2007).*

[2] *One example of this is the use of fixed or "hard-coded" values in an exploit, for example pointing to a single location memory (although this is a comparatively dated example). These fixed values can give defenders information to look for in other attacks, detecting the same exploit before it executes.*

[3] *Similarly, it is sometimes possible to combine several comparatively unexciting vulnerabilities into a highly effective production exploit.*

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

incredibly rare and can represent substantial investment by the malware's author (Bilge and Dumitras 2012).

There are a variety of actors searching daily for new vulnerabilities, contributing to what has become an arms race of sorts between these many researchers and vendors trying to secure their software products. Some of these vulnerabilities are found and quietly fixed within large software vendors like Google, or volunteers supporting open source software projects, while others are discovered by smaller security firms, academic groups, and independent security researchers (Keizer 2009; Finifter, Akhawe, and Wagner 2013; Goodin 2015). One of the key insights of increasingly public efforts to find vulnerabilities and disclose them to vendors is that a very small minority of these bug-hunters account for a large percentage of flaws discovered in software (The 2016 Bug Bounty Hacker Report 2016). Many of these efforts to discover vulnerabilities involve collaboration across borders. Defenders and researchers often take for granted the free flow of information across political boundaries and so would be stymied by restrictive export controls, like those found in Wassenaar.

The existence of a vulnerability is just information, like the coordinates of buried treasure on a map. Having found a vulnerability, the discoverer faces the dilemma of who to tell while keeping the bug's existence secret from everyone else. This secrecy is a chief source of the vulnerability's value. Nothing about the first discovery of a vulnerability prevents it from being found again and again by others, what is known as a bug collision or rediscovery (Ablon and Bogart 2017; Herr and Schneier 2017). This leads to a competitive environment where groups try to find vulnerabilities before each other and sell or disclose them. Often malicious actors will pay a good deal more than companies (Algarni and Malaiya 2014).

Contrasting Proliferation Processes

Many WMDs have a complicated production cycle. Nuclear weapons require precise machining and the procurement of specific radioactive materials. Proliferation in these materials and tools often involves a state in some capacity, through theft or sale, and an often-covert network of specialists and intermediaries. The links in this supply chain for WMD devices are thus highly fragile and subject to disruption. Malware by contrast is made up of information which is easy to move across borders. Even where experience, or special skills are required to assemble this information into working code, the barrier to entry is nothing like that for enriching fissile material. The key is that malware can come from anywhere and states do not have a monopoly on the knowledge or capability to develop it. The following section explores some of the contrasts between the two environments, focusing on the process of proliferation.

The PSI: The WMD Proliferation Model

The PSI is designed to address a key shortcoming in the architecture of international maritime law. There are only a few circumstances in which interdiction, stopping and boarding a ship at sea, is legal. Concerns that the vessel may be carrying WMD materials is not one of these (Belcher 2011). Setting out a statement of principles in the PSI under which such

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

Table 1 Intentional Proliferation Pathways

	Origin	
Recipient	**State**	**Non-state**
State	Cooperation and capacity building	Distributed R&D
Non-state	Proxy relationships	Malware ecosystem

interdiction can take place helps fill that gap. It also addresses a critical weakness in the proliferation cycle, especially for WMD. There are few places with the research or engineering capability to build, say, a binary nerve agent and integrate it into a dispersion device or mount it onto an intermediate range missile. This scarcity might be a knowledge issue, finding individuals qualified to work with dangerous chemicals, or lack of facilities. Few states possess the equipment and materials required to assemble a ballistic missile and even fewer the nuclear warhead to place on top.

Transfer of knowledge, materials, and tools between groups is a critical part of the proliferation process. International shipping is a prime means to move these resources and technology between countries. More than 70 percent of "destabilizing military equipment, dual use goods, and narcotics traffic" finds its way around the world on a cargo ship, often under what are known as Flags of Convenience or FOC (Nikitin 2012). FOC are a legal arrangement whereby a ship will fly the flag of another country, different from its country of ownership or place of origin thereby gaining different legal protections or operate under a less restrictive regulatory regime. Without the PSI, there were questions as to the legality of a US vessel stopping and seizing cargo from ships flying one of these FOC, often registered in Panama or Liberia. One of the first moves by U.S.A. upon establishing the PSI was to sign up most of the popular FOC states. This direct transfer is more difficult to trace within cybersecurity, highlighting several different paths of proliferation.

Intentional Proliferation

Within cybersecurity, intentional proliferation of malware involves direct intelligence support and transfer of software from one party to another. States have no monopoly on capabilities here. Non-state groups are a constant source of innovation on both offense and defense. Proliferation of malware can include a range of different types of information: from highly valuable software vulnerabilities to complete malicious software programs and the supporting infrastructure to covertly deploy them. The skills and capacity of groups on the receiving end of this proliferation can vary dramatically. Table 1 summarizes these four pathways, leading to a discussion of the remaining three.

State to Non-State Proliferation

The prototypical interaction may best be represented by the array of proxy relationships established between states and non-state groups e.g., between China and an array of economically focused criminal group (Penn 2015). The range of proliferation options span from sharing limited information about vulnerabilities in a target to wholesale transfer of the source code for

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

espionage and destructive malware. One of the prevalent challenges of the proliferation issue with malware is the lack of adequate empirical understanding of what behavior has already taken place.

State-to-State Proliferation

The state-to-state proliferation pathway might take place as part of a capacity building scheme, a military coalition, or other cooperative framework. While there are yet few good measures of state offensive or defensive cyber capability, it remains true that all states are not equal in this respect. There is a wide difference in the skill and capacity of UK versus the Sudan, as two examples. Some allies may find one partner with a more sophisticated program for military cyber operations, leading to the transfer of offensive malware or defensive information. This sort of state-to-state transfer might also take place as part of ongoing coordinated operations. Open source reporting indicates that Stuxnet, while originally developed by U.S.A., was shared with and saw some important modifications by Israel during the course of the two state's campaign against Iran's nuclear enrichment program (Zetter 2014). Future example might see state's loaning out products of their research and design processes or intelligence infrastructure in lieu of other forms of military assistance.

The Malware Ecosystem

Unlike WMD, or ballistic missiles, developing malicious software does not require sensitive materials or much in the way of specialized facilities. The PSI's target was often cargo ships where WMD components remain sensitive to discovery and disruption. Developing and deploying malware has no similar point of weakness. Instead, malware development and use takes place amongst a global network of buyers and sellers. Malware is bought, sold, traded, and sometimes stolen on a series of underground websites, forums, and social networks (Herr and Ellis, "Disrupting Malware Markets"; Herr and Ellis 2016). Different groups and individuals have roles in developing, selling, and using this software, depending on each other for information and competing for customers (Ablon, Libicki, and Golay 2014).

When one malware author innovates, others notice. The result is an environment where sellers specialize and buyers include criminal groups and governments. Adding in the original software vendors, who often supply cash in exchange for information about weaknesses in their code, and a variety of defensive actors and you have a malware ecosystem where the goods are a combination of simple components, sophisticated software, and extended customer-facing services (Grier et al. 2012; Thomas et al. 2015). Groups without the capacity to build their own malicious software can purchase it from others, everything from individual components to outsourcing every step of the process. States participate in this ecosystem too: Russian and U.S. intelligence agencies buy vulnerabilities while less capable states like Ethiopia and Sudan purchase off-the-shelf surveillance malware complete with training courses and easy to use interfaces (Fung 2013; Zetter 2015).

States can also provide malware components and information to other groups in order use them as proxy actors. This intentional proliferation more closely resembles the type of transfer of weapons components and materials addressed by the PSI. Although malware does not require special

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

resources to be developed, such software can include a wide range of different technical features and behaviors. Some groups—often advanced states like Russia, U.S.A., or Israel—have researched and tested new malicious capabilities which might not be known to other parties. Intentionally sharing these capabilities is a form of proliferation and one not well controlled by Wassenaar, which focused on companies and sales through exports rather than covert transfer (Herr 2016).

Non-State to State Proliferation

Most of the activity in this pathway takes place through the malware ecosystem described above with companies like Hacking Team or NSO group selling malware and associated support and training services to states without the capability or willingness to develop them internally (Currier and Marquis-Boire 2015; Marczak and Scott-Railton 2016). However, this category could also include the substantial development and support capacity sold from the defense contracting community to more capable states like the U.S.A. and U.K. (Boyd 2016; Northrop 2017). In addition to tools and direct technology transfer, there is also a substantial trade in vulnerability information and their associated PoC exploits from firms like Exodus Intelligence, Zerodium, and ReVuln (Wilson et al. 2016). It is also possible that some governments use criminal groups as an extended umbrella for research and development in exchange for legal protections (Sood and Enbody 2013; Goncharov 2014).

Unintentional Proliferation

In addition to the deliberate transfer of intentional proliferation, cybersecurity raises the possibility of unintentional proliferation, where malware's function or some properties are disclosed to a target or third parties during use. When a nuclear device or chemical weapon goes off, it leaves few pieces around for the target to pick over and reuse.[4] Malicious software leaves itself open to capture and analysis because it must be placed on the target and run successfully to work. This makes complicated malware designs and capabilities subject to far more effective forensic analysis than the comparable blast residue of a guided munition.

One of the major sources of innovation in the design and employment of non-state-authored malicious software comes from state-built code (Herr and Armbrust 2015; Buchanan 2017). Duqu, a likely state-built piece of espionage malware was discovered in 2011. This malware was used to exploit the Windows operating system to ensure its payload would function properly (Bonfante et al. 2013). Less than a year after its public discovery, the same exploit was integrated into two major criminal malware kits and used in attacks against a range of targets by criminal groups (Wolf 2013). This reuse of the originally state-authored exploit helped criminal groups to innovate and compromise more targets.

Code can also be stolen or compromised by other malicious actors. In 2015 the Italian firm, Hacking team, which sells surveillance malware, was breached and attackers made off with all of the company's data available online including e-mails and source code for the firm's products (Porup 2016).

[4]*There are instances where groups have stolen or recovered spent or improperly disposed of WMD materials. These cases would constitute unintentional proliferation but are extremely rare.*

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

Unlike the challenge of forensic analysis on a piece of malware that has been used against a target, these leaks of source code provide the software's blueprints in a form most readily intelligible and reusable by an analyst.[5] Available for download, exploits from the Hacking Team's product source code made its way into a variety of new pieces of malware. Demonstrating the directionless nature of this sort of unintentional proliferation, these exploits were also used by the defensive community to locate several previously unknown vulnerabilities and fix them (Paganini 2016; Zetter 2016). The year 2016 also saw the first overt leak of the source code for malware attributed to the American National Security Agency (Schneier 2016).

There are a variety of factors which influence the likelihood of malware's reuse and having possession of a malware sample does not make it possible to drag and drop its features into software. On obtaining a sample of malware, the analyst must rebuild the code. Because of the nature of software design, there are several forms code can take between its original authorship and running as a program. Analyzing a piece of malware, the analyst must reconstruct its function by watching how it runs on a computer, what behaviors it takes to manipulate the system, and how it spreads elsewhere. These behaviors, as well as some architectural details about the malware sample, can be obtained through a process known as reverse-engineering (Hoglund and McGraw 2004). This is a time-consuming effort filled with uncertainty and requires a great deal of skill. Importantly, it highlights that there are a range of different activities and software which might be restricted under a regime governing proliferation.

Proliferation in cybersecurity is not unique in grappling with dual use goods, uranium has long vexed policymakers as both source of fuel for civilian energy facilities and fissile material for nuclear weapons. The importance of information may be heightened here but, similarly, is not limited only to discussions of cyberspace; A.Q. Khan famously spent several years as research staff member at a Dutch-based facility designing new and more efficient ways to process nuclear material (Langewiesche 2005). The challenge for malicious software is that many of the component materials are embedded in everyday software and defensive activities such that to tug the way on one thread threatens to rend our collective connective fabric asunder. There are ways to govern the proliferation of malicious software but few focus solely on the code alone.

The Goals of Governing Proliferation

What are the goals of a regime to govern the content of proliferation or its process? Let us examine the two regimes we have defined earlier. First the PSI regime. We identified that the PSI involves a very light touch. One of the reasons for the PSI's relative light touch defining very little of what it seeks to control is to attract a wide number of member states. By reducing

[5]*Software can exist in several different forms. On its creation, in the bracketed syntax most of us are used to envisioning as "computer code". This source code is sequences of instructions written out in human intelligible form. From here, depending on the language in use, source code is compiled into object or "assembly" code. This may be human readable but without the same natural language state of Source. From here, this code must be assembled with any other files the program will depend on (libraries or other subsidiary programs) and assembled into machine code, which can be understood by the computer (http://stackoverflow.com/questions/466790/assembly-code-vs-machine-code-vs-object-code & https://www.cs.cmu.edu/~dst/DeCSS/object-code.txt).*

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

the requirements on participating states and leaving the end goals diffuse and subject to interpretation, there is less and less that potential members are likely to find disagreement over. Wassenaar, on the other hand has a much more specific definition of the software to be controlled but it similarly suffers from a multitude of goals. Some suggest Wassenaar was intended to serve human rights concerns as well as blocking the sale of surveillance malware to repressive regimes (Maurer and Kehl 2014). But the origins of the U.K. proposal, and much of the subsequent discussion in U.S.A., has centered on national security concerns.

The ambiguity in goals is especially challenging in cybersecurity as the private sector plays a bigger role than in any comparable WMD environment. Without clear aims the state's efforts are likely to flounder. It is largely companies that lay the fiber, own the microwave links, build the datacenters, and design the computing platforms involved. These same companies and non-state groups debate the standards and protocols which undergird all this computing and connectivity and it is private organizations who bear the brunt of the cost of insecurity in cyberspace. States will find it difficult to obtain cooperation from private sector groups without clarity of purpose.

The PSI: Goals and Scope

As noted earlier, the principal challenge embraced by the PSI was how to overcome the ambiguity in international law which would prevent the search and seizure of vehicles suspected of transporting WMD components. While the Initiative covers activities across air, land, and sea, the focus appears to have been on maritime interdiction where, "transshipment of WMD-related material for illicit purposes was not criminalized under international law, and there were limited legal grounds for seizure". The goal was thus to establish a very limited framework under which states could employ their own domestic laws to stop, search, and seize WMD devices and related components. This framework would also enhance information sharing between members and help drive the exchange of best practices.

Goals in Cybersecurity

Somewhat like the PSI, one of the principal limitations of the debate over malware proliferation has been the lack of clearly defined goals. This undercuts the ability to provide analysis as to the efficacy of proposals. Is national security the predominant interest, over human rights or governing foreign surveillance activates? Assuming national security is the dominant goal, is the predominant threat from states or non-state groups and is the response intended to deal with peacetime or conflict activity? One potential cause of these ambiguous goals may be the difficulty in distinguishing 'good' activities from 'bad'—the same information can be used maliciously or to patch and defend a computer system. The diversity of actors who build, buy, and sell malicious software, from the most advanced states to the least skilled criminal groups, makes the use of a single policy tool impractical.

The most prominent example of this is in distinguishing between the responsibilities of law enforcement and national-security-focused organizations. Criminal behavior emphasizes non-state actors with a wide variety of skill types whose legitimacy is generally poor. These groups are thus most easily subject to domestic laws and existing enforcement programs, at least

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

where they are domestic in origin and existence. Restricting behaviors, such as making it illegal to throw a stone through a store window, are well within the state's capacity and international cooperation to combat criminal behavior is challenging though not impossible.

National security goals, by contrast, tend to encompass the capabilities and behavior of states and some non-state groups less subject to criminal prosecution. Law enforcement tools are largely ineffective in restraining their activity. Altering the behavior of other states is likely to require some degree of self-restraint on the part of the target or coordinated action with others in the international system. Even then, it remains difficult to restrict these state's internal research and development activities. Unlike with chemical weapons, or nuclear research, there are few requirements in cybersecurity for specialized facilities or testing which might be externally visible, e.g., through air-sampling or seismic detection. Understanding this distinction between national security and criminal efforts, there are several goals which a governance regime aimed at proliferation might endeavor to accomplish.

Building Stability

While the existing efforts from Wassenaar to restrict malware sales remain mired in controversy, there are three goals in proliferation which might be possible and hold some merit. The first goal would prioritize global stability, the most audacious of the three. States may try to govern the proliferation of malware with an eye toward containing actors of concern and removing elements of uncertainty from crises. States are likely the focus here: the goal to set peacetime and in-conflict norms against targeting certain protected classes, like Computer Emergency Response Teams (CERTs) and civilian healthcare facilities. Efforts to improve stability could involve confidence building measures between states like U.S.A. and China. An example of this kind of effort could include: co-hosting vulnerability discovery competitions like Pwn2Own. Another might be: operating joint Internet security programs, for example remediating bugs like Heartbleed in widely used open source software. These efforts will encounter different challenges adapting an older regime to fit vice constructing something new but remain substantially challenging, as the process of norm development is quite a bit more than just pronouncing new behaviors (Finnemore and Hollis 2016).

Enhancing Cooperation and Common Understanding

A second goal would aim not to materially restrict the capabilities of states but use a governance regime to enhance the cooperation of willing states by developing shared expectations and subject matter expertise. This approach focuses less on governing proliferation directly, instead focusing more on building the competence of the government agents involved. This is more akin to the PSI's approach, which has succeeded most in sharing best practices and enhancing cooperation between members including trainings for less competent states (Dunne 2013; Williams 2013). The existing GGE at the UN contains elements of this idea but is: (1) temporary in nature; and (2) risks fragmentation from being structured as a naturally diverse consensus building body rather than a training and discussion forum. GGE may accomplish some of these goals, helping to build common understanding, but exists as a temporary measure rather than a permanent forum.

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

Drawing Battle Lines

Distinct from aiming for global stability or enhanced cooperation, a proliferation governance regime might be used as a tool to establish communities of interest and demarcate coalitions. Within the cyber norms debate, there are distinct negotiating positions on a range of issues from controls over the flow of information to the legitimacy of intellectual property as a target for espionage activities. U.S.A. worked to bring these disparate parties together, creating broader buy-in for the few points of consensus all share. The acknowledgement that international law applies to cyberspace, while it may have been a product of only temporary consensus, is regularly hailed as one of the chief points of progress in cybersecurity norms (Schmitt 2014; Fidler 2015). This strategy has also, perhaps intentionally, kept progress shallow and iterative making it difficult for competing states to shape consensus on contentious issues like censorship. The irony is that this slow pace of progress may well provide the impetus for smaller groups of like-minded states to coalesce around shared goals. The PSI is not a model of broad consensus, but rather a narrowly interested set of states with strong leadership from U.S.A. The accomplishment of the PSI has been to bring this group together to coordinate, and sometimes cooperate, on the interdiction of WMD components as defined by each individual member. A comparable model in cybersecurity would likely be similarly issue-based and the conclusion, below, suggests two possible approaches.

Conclusion

Malicious software does not look like nuclear weapons and so their respective governance regimes will differ. There is insight to be had about cybersecurity from comparing the two, largely in the goals and structure of the governing regime. Looking at the PSI and Wassenaar, this article asked three questions: what are the contents of proliferation; how does this proliferation take place; and what are the goals of the relevant governance regime? In examining these, the article concludes that the PSI is a poor model for counter-proliferation in cybersecurity owing to the broader challenges of interdicting malware.

The PSI has been moderately successful, with claims of interdictions in 2005 and 2006, for example, which might not otherwise have taken place (Belcher 2011). The Initiative has also facilitated capacity building in partner states and some information sharing. On this basis it could be judged a qualified success (Dunne 2013). By contrast, Wassenaar has instigated serious debate amongst stakeholders in the US, Europe, and Australia (Bratus et al. 2014; Little Limbago and Pierce 2015).[6] Unlike WMD components, malicious software does not lend itself well to transfer-focused controls.

What Could Come Next?

Common and Permissive Security Research Laws

Designing protections for good faith security research across U.S.A. and EU could help facilitate substantive dialogue as well as positive outcomes for the defensive security community. Protecting individuals' and organizations' ability to take software apart and search for vulnerabilities or design new defensive techniques creates benefits for those who defend computer

[6] *It should be noted that U.S.A. is the only state not to have implemented the controls and is actively engaged in pushing for their modification.*

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

systems. Crafting these rules also provides a basis for international collaboration between academics and researchers in the private sector. The content of negotiating the principles for these security research laws could also serve as useful vehicle for capacity building with less well-equipped states including strong involvement from private sector groups.

Attacking the Vulnerability Lifecycle

Rather than targeting malware transfer, a better approach may be to target the incentives attackers possess to develop this software and constrain the supply of software vulnerabilities by enhancing defender's attempts to fix (patch) software, rather than blocking the transfer of malware across borders. Enhancing financial benefits to companies and researchers to find and disclose software vulnerabilities and defensive techniques will more efficiently push this information to defensive organizations. This approach must go hand in hand with radically improved incentives for software companies and vendors to then develop and apply patches for these bugs. Many of these changes are regulatory and should take place at the domestic level. But while not explicitly an international regime, this approach creates opportunities for states to collaborate and share best practices as well as encourage cross-national vulnerability information sharing. As already pointed out, there are a number of means to deter attackers short of direct confrontation or limitation (Nye 2017). Increasing the difficulty of attackers by limiting the supply of these vulnerabilities is one such example.

Cybersecurity is a challenging area of inquiry, partly because it is an artificial agglomeration of issues—everything from crime to national security to the activities of civil society and the private sector. The challenge also stems from the perception that some advanced technical degree is required to understand the creation and use of code. There are certainly barriers to entry in understanding what software is and can do but there is also much more accessibility than is commonly understood. This is important because as the role of states in cybersecurity continues to grow, the insights of scholars in governance and other fields of study outside of computer science will be in ever greater demand. As well, practitioners must find a clear-eyed view of the possible and the useful. As the debate continues, hopefully this article may serve as some contribution to evaluating both.

Acknowledgements

Thank you to *Global Summitry* Senior Editor, Alan Alexandroff, the *Global Summitry* reviewers, Joseph Nye, Charley Snyder, and Rob Morgus for their comments. Additional thanks to the faithful fellows of the Harvard Cyber Security project including Annie Boustead, Ben Buchanan, and Scott Shackleford as well as Michael Sulmeyer, Jessica Malekos Smith and Kate Miller for their feedback. This work gratefully acknowledges support from the Belfer Family and the Flora and William Hewlett Foundation.

Works Cited

Aaron Boyd, "CYBERCOM Awards Spots on New $460M Cyber Operations Contract," *Federal Times*, May 23, 2016. http://www.federaltimes.com/story/government/cybersecurity/2016/05/23/cybercom-operations-contract/84787066/.

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

Ablon, Lillian, and Andy Bogart. 2017. *Zero days, thousands of nights*. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf.

Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay. 2014. *Markets for cybercrime tools and stolen data: Hackers' bazaar*. Rand Corporation. http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

Algarni, A., and Y. Malaiya. 2014. Software vulnerability markets: Discoverers and buyers. *International Journal of Computer, Information Science and Engineering* 8(3):71–81.

Anderson, Colin. 2015. *Considerations on Wassenaar arrangement control list additions for surveillance technologies*. Access. https://cda.io/r/ConsiderationsonWassenaarArrangementProposalsforSurveillanceTechnologies.pdf

Anderson, Justin, Thomas Devine, and Rebecca Gibbons. 2014. *Nonproliferation and counterproliferation*. http://www.oxfordbibliographies.com/display/id/obo-9780199743292-0026.

Arimatsu, Louise. 2012. A treaty for governing cyber-weapons: Potential benefits and practical limitations. In *Cyber Conflict (CYCON), 2012 4th International Conference on*, eds. Christian Czosseck, Rain Ottis, and Katharina Ziolkowski, 1–19. Tallinn, Estonia: IEEE. http://ieeexplore.ieee.org/abstract/document/6243968/

Becker, Georg T., Francesco Regazzoni, Christof Paar, and Wayne P. Burleson. 2013. *Stealthy dopant-level hardware trojans, August*. http://people.umass.edu/gbecker/BeckerChes13.pdf

Belcher, Emma. 2011. *The proliferation security initiative*. http://www.cfr.org/content/publications/attachments/IIGG_WorkingPaper6_PSI.pdf.

Bilge, Leyla, and Tudor Dumitras. 2012. Before we knew it: An empirical study of zero-day attacks in the real world. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, eds. Yu Ting, George Danezis, and Virgil Gligor, 833–44. New York, NY: ACM. http://dl.acm.org/citation.cfm?id=2382284

Bonfante, Guillaume, Jean-Yves Marion, Fabrice Sabatier, and Aurélien Thierry. 2013. Analysis and diversion of Duqu's driver. In *Proceedings of the 2013 8th International Conference on Malicious and Unwanted Software*, ed. Fernando C. Colon Osorio, 109–15. Fajardo, Puerto Rico: IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6703692

Bratus, Sergey, DJ Capelis, Michael Locasto, and Anna Shubina. 2014. *Why Wassenaar arrangement's definitions of intrusion software and controlled items put security research and defense at risk – and how to fix it*. Public Comment. http://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf.

Brian Fung, "The NSA Hacks Other Countries by Buying Millions of Dollars' Worth of Computer Vulnerabilities," *The Washington Post*, August 31, 2013. https://www.washingtonpost.com/news/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/

Bruce Schneier, "Major NSA/Equation Group Leak—Schneier on Security," *Schneier on Security*, August 16, 2016. https://www.schneier.com/blog/archives/2016/08/major_nsaequati.html.

Buchanan, Ben. 2017. *The Legend of Sophistication in Cyber Operations*. Cambridge, MA: Belfer Center, Harvard Kennedy School.

Christopher Bronk and Dan Wallach, "Opinion: Cyber Arms Control? Forget about It," *CNN*, March 26, 2013. http://www.cnn.com/2013/03/26/opinion/bronk-wallach-cyberwar/index.html.

Christopher Castelli, "Review Aimed at Framework for Cyber Stability Plows Familiar Ground," *Inside Cybersecurity*, July 8, 2014. http://securityassistance.org/south-asia/content/review-aimed-framework-cyber-stability-plows-familiar-ground.

Cora Currier and Morgan Marquis-Boire, "A Detailed Look at Hacking Team's Emails About Its Repressive Clients," *The Intercept*, July 7, 2015. https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

Corera, Gordon. 2006. *Shopping for Bombs: Nuclear Proliferation, Global Insecurity, and the Rise and Fall of the AQ Khan Network*. New York, NY: Oxford University Press. https://global.oup.com/academic/product/shopping-for-bombs-9780195375237?cc=us&lang=en&.

Dan Goodin, "All Four Major Browsers Take a Stomping at Pwn2Own Hacking Competition," *Ars Technica*, March 20, 2015. http://arstechnica.com/security/2015/03/all-four-major-browsers-take-a-stomping-at-pwn2own-hacking-competition/.

Data Breach Investigations Report (DBIR). 2015. *Verizon Enterprise Solutions*. http://www.verizonenterprise.com/DBIR/2015/ (accessed December 21, 2015).

DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven, CT: Yale University Press. https://books.google.com/books?hl=en&lr=&id=jfxfAgAAQBAJ&oi=fnd&pg=PA1&dq=denardis+internet+architecture&ots=gAzxUpHoEY&sig=1d9iufSQU0UxsUGeZl0MNIbtikU

Dullien, Thomas, Vincenzo Iozzo, and Mara Tam. 2015. *Surveillance, software, security, and export controls*. Public Comment. https://tac.bis.doc.gov/index.php/component/docman/doc_view/299-surveillance-software-security-and-export-controls-mara-tam?Itemid=.

Dunne, Aaron. 2013. *The proliferation security initiative: legal considerations and operational realities*. SIPRI Policy Paper, no. 36. Solna, Sweden: SIPRI, Stockholm International Peace Research Institute.

Durkalec, Jacek. 2012. *The Proliferation Security Initiative: Evolution and Future Prospects*. EU Non-Proliferation Consortium.

Fidler, David. 2015. *The UN GGE on cybersecurity: How international law applies to cyberspace.* Council on Foreign Relations–Net Politics April 14. http://blogs.cfr.org/cyber/2015/04/14/the-un-gge-on-cyber-issues-how-international-law-applies-to-cyberspace/.

Finifter, Matthew, Devdatta Akhawe, and David Wagner. 2013. "*An empirical study of vulnerability rewards programs*." USENIX Security. https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_finifter.pdf.

Finnemore, Martha, and Duncan B. Hollis. 2016. Constructing norms for global cybersecurity. *American Journal of International Law* 110(3):425–79. doi:10.1017/S0002930000016894.

Goldman, Emily O., and John Arquilla. 2014. *Cyber analogies*. DTIC Document. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA601645.

Goncharov, Max. 2014. *Russian underground revisited*. Cybercriminal Underground Economy Series. http://www.trendmicro.com.au/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf.

Grier, Chris, Lucas Ballard, Juan Caballero, Neha Chachra, Christian J. Dietrich, Kirill Levchenko, Panayiotis Mavrommatis, et al. 2012. Manufacturing compromise: The emergence of exploit-as-a-service. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, eds. Yu Ting, George Danezis, and Virgil Gligor, 821–32. New York, NY: ACM. http://dl.acm.org/citation.cfm?id=2382283

Gregg Keizer, "Single Code Typo Triggers Massive Internet Explorer Hack Attacks," *IT Business*, August 4, 2009. http://www.itbusiness.ca/news/single-code-typo-triggers-massive-internet-explorer-hack-attacks/13806.

Haq, Thoufique, Ned Moran, Sai Vashisht, and Mike Scott. 2013. "*Operation quantum entanglement.* FireEye Labs. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf.

Herr, Trey. 2014. PrEP: A framework for malware & cyber weapons. *The Journal of Information Warfare* 13(1):87–106.

—— 2016. Malware counter-proliferation and the Wassenaar arrangement. In *2016 8th International Conference on Cyber Conflict: Cyber Power*. 175–90, Tallinn, Estonia: IEEE. http://dx.doi.org/10.2139/ssrn.2711070

Herr, Trey, and Ellis Ryan. 2016. Disrupting Malware Markets. In *Cyber Insecurity: Navigating the Perils of the Next Information Age*, eds. Richard Harrison and Trey

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

Herr, Lanham, MD: Rowman & Littlefield, 2016), https://books.google.com/books?id=NAp7DQAAQBAJ&source.

Herr, Trey, and Bruce Schneier. 2017. *Taking stock: estimating vulnerability rediscovery*. Cyber Security Project Paper. Cambirdge, MA: Harvard Kennedy School, Belfer Center. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2928758

Herr, Trey, and Eric Armbrust. 2015. Milware: Identification and implications of state authored malicious software. In *NSPW '15 Proceedings of the 2015 New Security Paradigms Workshop*, 29–43. Twente, Netherlands: ACM. doi:10.1145/2841113.2841116.

Herr, Trey, and Paul Rosenzweig. 2015. Cyber weapons and export control: Incorporating dual use with the prep model. *Journal of National Security Law & Policy* 8(2): 301.

Hoglund, Greg, and Gary McGraw. 2004. *Exploiting Software: How to Break Code*. London, UK: Pearson Higher Education.

International Security Advisory Board. 2014. *Report on a framework for international cyber stability*. State Department. https://www.state.gov/t/avc/isab/229023.htm.

J.M. Porup, "How Hacking Team Got Hacked," *Ars Technica*, April 19, 2016. http://arstechnica.com/security/2016/04/how-hacking-team-got-hacked-phineas-phisher/.

King, Meg, and Robert Litwak. 2015. *Arms Control in Cyberspace*? *Wilson Briefs*. Washington, D.C.: The Wilson Center.

Koch, Susan J. 2012. *Proliferation security initiative: origins and evolution*. DTIC Document. Washington, D.C.: National Defense University. http://www.dtic.mil/get-tr-doc/pdf?AD=ADA577517.

Langewiesche, William, "The Wrath of Khan," *The Atlantic*, November 2005. https://www.theatlantic.com/magazine/archive/2005/11/the-wrath-of-khan/304333/.

Larsen, Jeffrey Arthur, and James M. Smith. 2005. *Historical Dictionary of Arms Control and Disarmament*. Lanham, MD: Scarecrow Press.

Lewis, Jim, and Vignard Kerstin. 2016. *Report of the International Security Cyber Issues Workshop Series 656*. UNIDIR and CSIS. http://www.unidir.org/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf.

Lipson, Michael. 1999. The reincarnation of CoCom: Explaining post-cold war export controls. *The Nonproliferation Review* 6(2):33–51.

Little Limbago, Andrea, and Cody Pierce. 2015. *Much ado about Wassenaar: The overlooked strategic challenges to the Wassenaar arrangement's implementation*. https://www.endgame.com/blog/much-ado-about-wassenaar-overlooked-strategic-challenges-wassenaar-arrangement%E2%80%99s-implementation.

MacCalman, Molly. 2016. AQ Khan nuclear smuggling network. *Journal of Strategic Security* 9(1):104–18.

Marczak, Bill and John Scott-Railton. 2016. "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used against a UAE Human Rights Defender," *The Citizen Lab* August 24, 2016. https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

Mastanduno, Michael. 1992. *Economic Containment: CoCom and the Politics of East-West Trade*. Cornell, NY: Cornell University Press.

Michael N. Schmitt. 2014. *Tallinn Manual on the International Law Applicable to Cyber Warfare. Humanitarian Law*. Cambridge, UK: Cambridge University Press. http://www.cambridge.org/us/academic/subjects/law/humanitarian-law/tallinn-manual-international-law-applicable-cyber-warfare (accessed August 21, 2014).

Microsoft. 2007. *VBS.LOVELETTER worm virus*. http://support.microsoft.com/kb/282832.

Mueller, Milton. 2004. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT Press.

Nick Espinoza, "Prove It: The Rapid Rise of 12,000 Shared Proof-of-Concept Exploits," *Recorded Future*, May 5, 2016. https://www.recordedfuture.com/shared-poc-exploits/.

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

Nikitin, Mary Beth. 2012. *Proliferation Security Initiative (PSI). RL 34327*. Congressional Research Service. https://fas.org/sgp/crs/nuke/RL34327.pdf

Northrop Gruman. 2017. *Northrop Grumman awarded cyber security contract by UK government*. Press Release. https://www.northropgrummaninternational.com/northrop-grumman-awarded-cyber-security-contract-by-uk-government/ (accessed January 6, 2017).

Nye, Joseph S. 2011. Nuclear lessons for cyber security? *Strategic Studies Quarterly*, 5(4): 18–38.

——— 2017. Deterrence and dissuasion in cyberspace. *International Security* 41(3):44–71.

O'Neill, Maire. 2016. Insecurity by design: Today's IoT device security problem. *Engineering, Special Section: The Grand ChallengesExecutive Associate EditorsMembersSpecial Section: Nuclear PowerMembersGuest Editors-in-ChiefGuest Editors-in-Chief* 2(1):48–9. doi:10.1016/J.ENG.2016.01.014.

Penn, Megan. 2015. Organized Cyber Crime: Comparison of Criminal Groups in Cyberspace. *Cyber Defense Review*, 2015. http://cyberdefensereview.army.mil/The-Journal/Article-Display/Article/1136136/organized-cyber-crime-comparison-of-criminal-groups-in-cyberspace/.

Pierluigi Paganini, "Dogspectus Ransomware Campaign Relies on Leaked Hacking Team Exploits and Towelroot," *Security Affairs*, April 26, 2016. http://securityaffairs.co/wordpress/46693/malware/dogspectus-android-ransomware.html.

Rami Kogan, "Bedep Trojan Malware Spread by the Angler Exploit Kit Gets Political," *Trustwave*, April 29, 2015. https://www.trustwave.com/Resources/SpiderLabs-Blog/Bedep-trojan-malware-spread-by-the-Angler-exploit-kit-gets-political/

Ramilli, Marco, and Matt Bishop. 2010. Multi-stage delivery of malware. In *Malicious and Unwanted Software (MALWARE), 2010 5th International Conference on*, ed. Fernando C. Colon Osorio, 91–7. Nancy, France: IEEE. http://ieeexplore.ieee.org/abstract/document/5665788/.

Rollins, John W. 2015. *U.S.–China Cyber Agreement. IN10376*. Congressional Research Service. https://fas.org/sgp/crs/row/IN10376.pdf.

Shackelford, Scott. 2009. From nuclear war to net war: Analogizing cyber attacks in international law. *Berkeley Journal of International Law* 25(3). https://papers.ssrn.com/abstract=1396375.

Sood, Aditya K., and Richard J. Enbody. 2013. Crimeware-as-a-service—A survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection* 6(1):28–38. doi:10.1016/j.ijcip.2013.01.002.

Sterner, Eric. 2015. *Obama's Welcome Cyber Sanctions Plan is worth expanding*, April 8. http://www.worldpoliticsreview.com/articles/15480/obama-s-welcome-cyber-sanctions-plan-is-worth-expanding.

The 2016 Bug Bounty Hacker Report. 2016. *HackerOne*. https://hackerone.com/blog/bug-bounty-hacker-report-2016.

Thomas, Hurt, Danny Huang, David Wang, Elie Bursztein, Chris Grier, Thomas J. Holt, Christopher Kruegel, Damon McCoy, Stefan Savage, and Vigna. 2015. *Framing dependencies introduced by underground commoditization*. http://damonmccoy.com/papers/WEIS15.pdf.

Tim Maurer and Danielle Kehl, "Against Hypocrisy: Updating Export Controls for the Digital Age," *Cyber Dialogue Conference*, May 2, 2014. http://www.cyberdialogue.ca/2013/03/against-hypocrisy-updating-export-controls-for-the-digital-age-by-danielle-kehl-and-tim-maurer/.

Williams, Ian. 2013. *Proliferation security initiative: Ten years on*, May 28. https://armscontrolnow.org/2013/05/28/proliferation-security-initiative-ten-years-on/.

Wilson, Andi, Ross Schulman, Kevin Bankston, and Trey Herr. 2016. *Bugs in the system*. New America Open Technology Institute. https://na-production.s3.amazonaws.com/documents/Bugs-in-the-System-Final.pdf.

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020

Wolf, Julia. 2013. *CVE-2011-3402 – Windows kernel truetype font engine vulnerability (MS11-087)*, presented at the CanSecWest, March 8. https://cansecwest.com/slides/2013/Analysis%20of%20a%20Windows%20Kernel%20Vuln.pdf.

Zetter, Kim. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York, NY: Crown/Archetype.

——. 2015. "Hacking Team Leak Shows How Secretive Zero-Day Exploit Sales Work," *Wired*, July 24, 2015. http://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/.

——. 2016. "Hacking Team's Leak Helped Researchers Hunt Down a Zero-Day," *Wired* January 13, 2016. https://www.wired.com/2016/01/hacking-team-leak-helps-kaspersky-researchers-find-zero-day-exploit/.

Zucker, Jessica. 2015. "US and China Reach Historic 'Cyber Arms Control Agreement' – But Will Anything Come of It?". *Kennedy School Review* October 2. http://harvardkennedyschoolreview.com/us-and-china-reach-historic-cyber-arms-control-agreement-but-will-anything-come-of-it/.

Downloaded from https://academic.oup.com/globalsummitry/article-abstract/3/1/86/3920644 by guest on 16 June 2020